PIN VERIFICATION USING CIPHER BLOCK CHAINING

W. Dale Hopkins
Steven W. Wierenga
Ching-Hsuan Chen
Jack Schifando

ABSTRACT

A PIN verification apparatus comprises a plurality of cipher blocks linked in a Cipher Block Chain (CBC) and keyed with a secret PIN Verification Key (PVK). A first input block is coupled to a first cipher block in the CBC chain and is configured to receive a plaintext block derived from a secret PIN. A second input block is coupled to a second cipher block in the CBC chain capable of receiving a plaintext block derived from a non-secret entity-identifier and ciphertext from a cipher block in the CBC chain.